Basic Axioms and Examples

Note 1

Given a set G, {{c2: a binary operation $\star$ on G}} is {{c1: a function

$$\star : G \times G \to G.$$

}}

Note 2

Given a binary operation $\star$ on a set G, for any $a, b \in G$ we shall write {{c2: $a \star b$}} for {{c1: $\star(a, b)$.}}

Note 3

A binary operation $\star$ on a set G is {{c2: associative}} if {{c1: for all $a, b, c \in G$ we have

$$a \star (b \star c) = (a \star b) \star c.$$

}}

Note 4

If $\star$ is a binary operation on a set G we say elements a and b of G {{c1: commute}} if {{c2:

$$a \star b = b \star a.$$

}}

Note 5

A binary operation $\star$ on a set G is {{c2: commutative}} if {{c1: for all $a, b \in G$ we have
$$a \star b = b \star a.$$

}}

Note 6

Suppose that $\star$ is a binary operation on a set G and $H \subseteq G$. If {{c2: the restriction of $\star$ to H is a binary operation on H,}} then H is said to be {{c1: closed under $\star$.}}

Note 7

{{c3::A group}} is {{c2::an ordered pair $(G, \star)$}} where {{c1::G is a set and $\star$ is a binary operation on G}} satisfying {{c4::the group axioms.}}

Note 8

How many axiom are there in the definition of a group $(G, \star)$?

❚ Three.

Note 9

What is the first axiom from the definition of a group $(G, \star)$?

❚ $\star$ is associative.

Note 10

Given a binary operation $\star$ on a set G, {{c3::an element $e \in G$}} is called {{c2::an identity of G}} if {{c1::for all $a \in G$ we have

$$a \star e = e \star a = a.$$

}}

Note 11

What is the second axiom from the definition of a group $(G, \star)$?

❚ There exists an identity of G.

Note 12

Given a binary operation $\star$ on a set G and $a \in G$, {{c3::an element $\tilde{a} \in G$}} is called {{c2::an inverse of a}} if {{c1::

$$a \star \tilde{a} = \tilde{a} \star a = e.$$

}}

Note 13

Given a binary operation $\star$ on a set G and $a \in G$, an inverse of a is usually denoted a^{-1}.

Note 14

What is the third axiom from the definition of a group $(G, \star)$?

❚ For all $a \in G$ there exists a^{-1}.

Note 15

A group $(G, \star)$ is called abelian if $\star$ is commutative.

Note 16

We shall say G is a group under $\star$ if $(G, \star)$ is a group.

Note 17

We shall say a set G is a group if G is a group under an operation that is clear from the context.

Note 18

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are groups under $+$.

Note 19

$\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$ are groups under $\times$.

Note 20

$\mathbb{Q}^{+}, \mathbb{R}^{+}$ are groups under $\times$.

Note 21

Is $\mathbb{Z} - \{0\}$ a group under $\times$?

❚ No. (There is no inverse.)

Note 22

Let V be a vector space. Then V is {{c2::a group}} under {{c1::$+$.}}

Note 23

Let $n \in \mathbb{Z}^+$. Then {{c3::$\mathbb{Z}/n\mathbb{Z}$}} is {{c2::a group}} under {{c1::addition}} of residue classes.

Note 24

Let $n \in \mathbb{Z}^+$. Then {{c3::$(\mathbb{Z}/n\mathbb{Z})^\times$}} is {{c2::a group}} under {{c1::multiplication}} of residue classes.

Note 25

If $(A, \star)$ and $(B, \diamond)$ are {{c4::groups,}} then the group {{c2::$A \times B$,}} whose operation is {{c1::defined componentwise:

$$(a, b)(c, d) = (a \star c, b \diamond d),$$

}} is called {{c3::the direct product of the two groups.}}

Note 26

If $(G, \star)$ is a group, then {{c2::the identity of G}} is {{c1::unique.}}

Note 27

If $(G, \star)$ is a group, then the identity of G is unique. What is the key idea in the proof?

▍ Consider the product of two arbitrary identities.

Note 28

If $(G, \star)$ is a group, then for every $a \in G$, {{c2::a^{-1}}} is {{c1::uniquely determined.}}

Note 29

If $(G, \star)$ is a group, then for every $a \in G$, a^{-1} is uniquely determined. What is the key idea in the proof?

▌ Multiply an inverse on the right by $a \star a^{-1}$.

Note 30

If $(G, \star)$ is a group and $a \in G$, then

$$(a^{-1})^{-1} = {}_{\{\{c1::}a.\}\}}$$

Note 31

If $(G, \star)$ is a group and $a, b \in G$, then

$$_{\{\{c2::}}(a \star b)^{-1}{}_{\}\}} = {}_{\{\{c1::}}(b^{-1}) \star (a^{-1}).{}_{\}\}}$$

Note 32

If $(G, \star)$ is a group and $a_1, \ldots, a_n \in G$, then the value of

$$a_1 \star \cdots \star a_n$$

is {{c2::independent}} of {{c1::how the expression is bracketed.}}

«{{c3::The generalized associative law}}»

Note 33

What is the key idea in the proof of the generalized associative law for a group $(G, \star)$?

▌ By induction.

Note 34

Henceforth our abstract groups G, H, *etc.* will always be written with the operation as {{c1::·.}}

Note 35

Henceforth for an abstract group G (operation $\cdot$) an expression $a \cdot b$ will always be written as ab.

Note 36

Henceforth for an abstract group G (operation $\cdot$) we denote the identity of G by 1.

Note 37

For any group G and $x \in G$ and $n \in \mathbb{Z}^+$ we shall denote by x^n the product

$$\underbrace{xx \cdots x}_{n \text{ terms}}.$$

Note 38

For any group G and $x \in G$ and $n \in \mathbb{Z}^+$ we shall denote by x^{-n} the product

$$\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}}.$$

Note 39

For any group G and $x \in G$, let $x^0 \overset{\text{def}}{=} 1$, the identity of G.

Note 40

Let G be a group and let $a, u, v \in G$. Then $au = av$ if and only if $u = v$.

«Cancellation rule»

Note 41

ed8673154d544c7b86ac358facc79101

For G a group and $x \in G$ define the order of x to be the smallest positive integer n such that

$$x^n = 1.$$

Note 42

8c334a6360be4bee8fae7f712ab2c4ee

For G a group and $x \in G$, if no positive power of x is the identity, the order of x is defined to be infinity.

Note 43

ba4143a322564f8383f6e7d91ca32a75

For G a group and $x \in G$, denote the order of x by $|x|$.

Note 44

d7fee5bcbdbd47bcb6f4a2ba086fa2ed

For G a group and $x \in G$, if the order of x is an integer n, x is said to be of order n.

Note 45

db12c606699d40e89d499d554bd52b28

For G a group and $x \in G$, if the order of x is infinite, x is said to be of infinite order.

Note 46

2e514c62ce4e48eb9c6bd3b5de1d7c44

An element of a group has order 1 if and only if it is the identity.

Note 47

babeb7cf1b394be6a4f8d86e1a099cda

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the matrix

$$\left[g_i g_j \right] \sim n \times n.$$

Note 48

f245736b42b44f178f9a1d661bc4a5c7

Let $G = \{x \in \mathbb{R} \mid x \in [0, 1)\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$. Then the group $(G, \star)$ is called the real numbers mod 1.

Note 49

3664191737c844f38816547b7acd64c1

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Then the group $(G, +)$ is called the group of roots of unity in $\mathbb{C}$.

Note 50

85c981d4f1564164bb547096829d245b

A finite group is abelian if and only if its group table is a symmetric matrix.

Note 51

859ef5188ad14b35b58dc9428333e5ad

Let G a group and $x \in G$ and $a, b \in \mathbb{Z}$. Then $x^{a+b} = x^a x^b$.

Note 52

0c6c419e61fc48139ff6afd4a8e28be6

Let G a group and $x \in G$. Then $|x^{-1}| = |x|$.

Note 53

f221410dc76e4c7881175d62226ecdf4

Let G a group and $x, g \in G$. Then $|g^{-1}xg| = |x|$.

Note 54

9951f3d62ec841df9c6f8cfc07f3c04f

Let G a group and $a, b \in G$. Then $|ba| = |ab|$.

Note 55

b30a94de99fe4c2f91b5417fdbb3e99d

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $x^s = 1$ if and only if $n \mid s$.

Note 56

5a0539b7021242e2a9a5769a1c156889

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then

$$|x^s| = \frac{n}{(n, s)}.$$

Note 57

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $|x^s| = \frac{n}{(n,s)}$. What is the key idea in the proof?

▌ $(x^s)^k = 1$ if and only if $n \mid sk$.

Note 58

Let G a group, $x \in G$. If $x^2 = 1$ then

$$x^{-1} = x.$$

Note 59

Let G a group. If a and b are commuting elements of G then $(ab)^n = a^n b^n$.

Note 60

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is abelian.

Note 61

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is abelian. What is the key idea in the proof?

▌ $1 = (ab)^2$ and multiply by a on the left and by b on the right.

Note 62

Let $(G, \star)$ be a group and $H \subseteq G$. If H is a group under the operation $\star$ restricted to H then H is called a subgroup of G.

Note 63

Let $(G, \star)$ and $H \subseteq G$. We shall say H is closed under inverses if for all $h \in H$ we have $h^{-1} \in H$.

Note 64

Let $(G, \star)$ be a group and $H \subseteq G$ be nonempty. If H is closed under $\star$ and inverses, then H is a subgroup of G.

Note 65

Let G a group and $x \in G$. Then the subgroup $\{x^n \mid n \in \mathbb{Z}\}$ of G is called the cyclic subgroup of G generated by x.

Note 66

Let A and B be groups. Then $A \times B$ is abelian if and only if both A and B are abelian.

Note 67

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Note 68

Let A and B be groups, $(a, b) \in A \times B$. Then

$$(a, b)^k = (a^k, b^k)$$

for all $k \in \mathbb{Z}$.

Note 69

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$. What is the key idea in the proof?

▎ $(a, b)^k = (a^k, b^k)$.

Note 70

Any finite group of even order contains an element of order 2.

Note 71

Any finite group of even order contains an element of order 2. What is the key idea in the proof?

Show that the set $\{g \in G \mid g \neq g^{-1}\}$ has an even number of elements.

Note 72

Let G a group, $x \in G$ and $|x| = n < \infty$. Then the elements {{c2::

$$1, x, x^2, \ldots, x^{n-1}$$

}} {{c1::are distinct.}}

Note 73

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x|$ {{c2:: $\leq$ }}{{c1:: $|G|$ }}.

Note 74

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x| \leq |G|$. What is the key idea in the proof?

The elements $1, x, \ldots, x^{n-1}$ are the only powers of x.

Note 75

Let G a group, $x \in G$ and $|x| = \infty$. Then the elements {{c2::

$$x^n, n \in \mathbb{Z}$$

}} {{c1::are distinct.}}

Dihedral Groups

Note 1

A symmetry of a regular n-gon is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

Note 2

Each symmetry of a regular n-gon can be described uniquely by the corresponding permutation of $\{1, 2, \ldots, n\}$, representing the permutation of the vertices.

Note 3

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, the group of symmetries of a regular n-gon is called the dihedral group of order $2n$.

Note 4

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, the dihedral group of order $2n$ is denoted D_{2n}.

Note 5

Given $n \in \mathbb{Z}^+, n \geq 3$ and $s, t \in D_{2n}$, the product st is defined to be the symmetry obtained by first applying t then s to the n-gon.

Note 6

Given $n \in \mathbb{Z}^+$ and $n \geq 3$,

$$|D_{2n}| = 2n.$$

Note 7

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, $|D_{2n}| = 2n$. What is the key idea in the proof?

> Every symmetry is uniquely determined by how it affects some two adjacent vertices.

Note 8

For convenience, the regular n-gon viewed in D_{2n} is fixed {{c1:: centered at the origin.}}

Note 9

For convenience, the vertices of the regular n-gon viewed in D_{2n} are labeled {{c1:: consecutively from 1 to n in a clockwise manner.}}

Note 10

In the context of the D_{2n} group, let {{c2::r}} be {{c1:: the rotation clockwise about the origin through $2\pi/n$ radian.}}

Note 11

In the context of the D_{2n} group, let {{c2::s}} be {{c1:: the reflection about the line of symmetry through vertex 1 and the origin.}}

Note 12

In the context of the D_{2n} group, is it possible that $s = r^i$ for some i?

> No.

Note 13

In the context of the D_{2n} group, is it possible that $sr^i = sr^j$ for some $i \not\equiv j \pmod{n}$?

❚ No.

Note 14

Each element of D_{2n} can be written {{c2::uniquely}} in the form {{c1:: $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n - 1$.}}

Note 15

In the context of the D_{2n} group,

$$r^i s = {}_{\{\{c1::}} sr^{-i}, {}_{\}\}} \text{ for } {}_{\{\{c2::}} \text{all } 0 \leq i \leq n \}\}.$$

Note 16

In the context of the D_{2n} group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

What is the key idea in the proof?

❚ $rs = sr^{-1}$ and by induction.

Note 17

{{c3::A subset S of elements}} of a group G with the property that {{c1::every element of G can be written as a (finite) product of elements of S and their inverses}} is called {{c2::a set of generators of G.}}

Note 18

If S is {{c2::a set of generators}} of a group G, we shall write {{c1::

$$G = \langle S \rangle.$$

}}

Note 19

If S is {{c2::a set of generators}} of a group G, we shall say G is {{c1::generated by S.}}

Note 20

In terms of generators, the group $D_{2n} = \langle r, s \rangle$.

Note 21

In a finite group G a set S generates G if every element of G is a finite product of elements of S.

Note 22

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any any other relation between elements of the group may be derived from these three.

Note 23

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any any other relation between elements of the group may be derived from these three. What is the key idea in the proof?

> We can determine exactly when two group elements are equal by using only these three relations.

Note 24

Let G be a group. Any equations in G that the generators satisfy are called relations in G.

Note 25

Let G be a group. If G is generated by a subset S and there is some collection of relations such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a presentation of G.

Note 26

Let G be a group. If a subset S and a collection of relations $R_1, \ldots, R_m$ form a presentation of G, we shall write

$$G = \langle S \mid R_1, \ldots, R_m \rangle.$$

Note 27

One presentation of the dihedral group D_{2n} is

$$D_{2n} = \left\langle r, s \mid r^n = s^2 = 1, \ rs = sr^{-1} \right\rangle.$$

Note 28

If $n = 2k$ is even and $n \geq 4$ then r^k is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.

Symmetric Groups

Note 1

Given a set Ω, the set of all bijections from Ω to itself is denoted S_Ω.

Note 2

Let Ω be a nonempty set. Then the group $\left(S_\Omega, \circ \right)$ is called the symmetric group on the set Ω.

Note 3

Let $n \in \mathbb{Z}^+$. The symmetric group on the set $\{1, 2, \ldots, n\}$ is called the symmetric group of degree n.

Note 4

Let $n \in \mathbb{Z}^+$. The symmetric group of degree n is denoted S_n.

Note 5

Let $n \in \mathbb{Z}^+$. Then

$$|S_n| = n!.$$

Note 6

A cycle is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).

Note 7

The cycle $(a_1 \ a_2 \ \ldots \ a_m)$ in S_n is the permutation

$$a_i \mapsto a_{i+1} \qquad a_m \mapsto a_1.$$

Note 8

{{c2: The length}} of a cycle in S_n is {{c1: the number of integers that appear in it.}}

Note 9

{{c2: A cycle of length t}} in S_n is called {{c1: a t-cycle.}}

Note 10

Two cycles in S_n are called {{c2: disjoint}} if {{c1: they have no numbers in common.}}

Note 11

Let $\sigma \in S_n$. {{c1: The representation of σ as the products of pairwise disjoint cycles}} is called {{c2: the cycle decomposition of σ.}}

Note 12

{{c2: The identity permutation}} of S_n will be written as {{c1: 1.}}

Note 13

S_n is a {{c2: non-abelian}} group for {{c1: all $n \geq 3$.}}

Note 14

{{c2: Disjoint}} cycles in S_n {{c1: commute.}}

Note 15

{{c3: The cycle decomposition}} of each permutation in S_n is the {{c1: unique}} way of expressing a permutation as {{c2: a product of disjoint cycles (up to rearrangement.)}}

Note 16

{{c3: The order}} of a permutation in S_n is the {{c2: l.c.m.}} of {{c1: the lengths of the cycles in its cycle decomposition.}}

Note 17

Let σ be a k-cycle in S_n. Then

$$|\sigma| = {\scriptstyle \{\{c1::}} k. {\scriptstyle \}\}}$$

Note 18

Let σ be a k-cycle in S_n. For which positive integers i is σ^i also a k-cycle?

▎ For i relatively prime to k.

Note 19

Let σ be a k-cycle in S_n. What is special about the cyclic decomposition of σ^i for an arbitrary $i \in \mathbb{Z}^+$?

▎ All of the disjoint cycles have the same length and are "evenly spaced."

Note 20

Let p be {{c3::a prime.}} An element has order {{c2::p}} in S_n if and only if {{c4::its cycle decomposition}} is {{c1::a product of commuting p-cycles.}}

Note 21

$${\scriptstyle \{\{c4::}} S_3 {\scriptstyle \}\}} = \langle a, b \mid {\scriptstyle \{\{c1::}} a^2 = b^2 = 1, {\scriptstyle \}\}} {\scriptstyle \{\{c2::}} aba = bab {\scriptstyle \}\}} \rangle,$$

where $a = {\scriptstyle \{\{c3::}} (1\ 2) {\scriptstyle \}\}}$, $b = {\scriptstyle \{\{c3::}} (2\ 3) {\scriptstyle \}\}}$.

Matrix Groups

Note 1

First, a field is {{c2: a set F}} together with {{c1: two binary operations $+$ and $\cdot$ on F.}}

Note 2

How are the properties of $+$ summarised in the definition of a field F?

▌ $(F, +)$ is an abelian group.

Note 3

How are the properties of $\cdot$ summarised in the definition of a field F?

▌ $(F - \{0\}, \cdot)$ is an abelian group.

Note 4

In the definition of a field F, what does 0 refer to?

▌ The identity of F with respect to $+$.

Note 5

What is the key property that relates $+$ and $\cdot$ in the definition of a field F?

▌ The distributive law.

Note 6

The distributive law from the definition of a field F states that

{{c1::

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

}}

Note 7

For any field F let $F^{\times} = F - \{0\}$.

Note 8

Given a prime p, we shall denote the field $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$ to emphasize that it is a field.

Note 9

Given $n \in \mathbb{Z}^{+}$ and a field F, the general linear group of degree n is denoted

$$GL_n(F).$$

Note 10

What are the elements of $GL_n(F)$?

> All $n \times n$ matrices whose entries come from a field F and whose determinant is nonzero.

Note 11

What is the operation of $GL_n(F)$?

> Matrix multiplication.

Note 12

Let F be a field. If $|F| < \infty$, then

$$|F| = p^m \quad \text{for some prime } p \text{ and an integer } m.$$

Note 13

Let F be a field. If $|F| = q < \infty$, then

$$|GL_n(F)| = \prod_{k=0}^{n-1} (q^n - q^k).$$

Note 14

Let F be a field. The subgroup of all the unit upper triangular matrices in $GL_3(F)$ is called the Heisenberg group over F.

Note 15

Let F be a field. The Heisenberg group over F is denoted $H(F)$.

Note 16

Let F be a field. Then

$$|H(F)| = |F|^3.$$

Note 17

Let $x \in H(\mathbb{R})$. If $x \neq 1,$ then

$$|x| = \infty.$$

The Quaternion Group

Note 1

The quaternion group is denoted Q_8.

Note 2

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Note 3

$$|Q_8| = 8.$$

Note 4

In Q_8, $\quad 1 \cdot x = x \cdot 1 = x, \quad$ for all x.

Note 5

In Q_8, $\quad (-1) \cdot x = x \cdot (-1) = -x, \quad$ for all x.

Note 6

In Q_8, $\quad (-1) \cdot (-1) = 1.$

Note 7

In Q_8, $\quad i \cdot i = -1.$

Note 8

In Q_8, $\quad j \cdot j = -1.$

Note 9

In Q_8, $\quad k \cdot k = -1.$

Note 10

In Q_8, $\quad i \cdot j = k.$

Note 11

In Q_8, $\quad j \cdot k = i$.

Note 12

In Q_8, $\quad k \cdot i = j$.

Note 13

In Q_8, $\quad j \cdot i = -k$.

Note 14

In Q_8, $\quad k \cdot j = -i$.

Note 15

In Q_8, $\quad i \cdot k = -j$.

Note 16

$$Q_8 = \langle i, j \rangle$$

Note 17

$$Q_8 = \langle i, j \mid i^2 = j^2, \ ij = ji^{-1} \rangle.$$

Homomorphisms and Isomorphism

Note 1

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \qquad \text{for all } x, y \in G$$

is called a homomorphism.

Note 2

Let G and H be groups. A map $\varphi : G \to H$ is called an isomorphism if it is a bijective homomorphism.

Note 3

Let G and H be groups. G and H are said to be isomorphic or of the same isomorphism type if there exists an isomorphism $G \to H$.

Note 4

Let G and H be groups. If G and H are isomorphic we shall write

$$G \cong H.$$

Note 5

Let $\mathcal{G}$ be a nonempty collection of groups. Then $\cong$ is an equivalence relation on $\mathcal{G}$.

Note 6

Let $\mathcal{G}$ be a nonempty collection of groups. The equivalence classes of $\cong$ are called isomorphism classes.

Note 7

The map $x \mapsto e^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

Note 8

The isomorphism type of a symmetric group depends only on the cardinality of the underlying set being permuted.

Note 9

Let Δ and Ω be nonempty sets. Then $S_\Delta \cong S_\Omega$ if and only if

$$|\Delta| = |\Omega|.$$

Note 10

Let Δ and Ω be nonempty sets. Then $S_\Delta \cong S_\Omega$ if $|\Delta| = |\Omega|$. What is the key idea in the proof?

▌ Build an isomorphism using a bijection $\Delta \to \Omega$.

Note 11

Let Δ and Ω be nonempty sets. Then $S_\Delta \cong S_\Omega$ if $|\Delta| = |\Omega|$. In the proof, how do we define the isomorphism φ?

▌ $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$, where $\theta : \Delta \to \Omega$ is a bijection.

Note 12

Theorems that determine what properties of a structure specify its isomorphism type are referred to as classification theorems.

Note 13

If $\varphi : G \to H$ is a group isomorphism, then

$$|G| = |H|.$$

Note 14

If $\varphi : G \to H$ is a group isomorphism, then

$$H \text{ is abelian if and only if } G \text{ is abelian.}$$

Note 15

If $\varphi : G \to H$ is a group isomorphism and $x \in G$, then

$$|\varphi(x)| = |x| .$$

Note 16

Let G and H be groups, $|G| < \infty,$ and

$$G = \langle s_1, \ldots, s_m \mid R_1, \ldots, R_k \rangle,$$
$$\{r_1, \ldots, r_m\} \subseteq H.$$

If any relation R_j is satisfied in H when each s_i is replaced by $r_i,$ then there is a unique homomorphism

$$\varphi : G \to H, \quad s_i \mapsto r_i.$$

Note 17

Let G and H be groups, $|G| < \infty$, and

$$G = \langle s_1, \ldots, s_m \mid R_1, \ldots, R_k \rangle,$$
$$\{r_1, \ldots, r_m\} \subseteq H,$$
$$\varphi : s_i \mapsto r_i \text{ be a homomorphism.}$$

If H is generated by $\{r_1, \ldots, r_m\},$ then φ is surjective.

Note 18

Let G and H be groups, $|G| < \infty$, and

$$G = \langle s_1, \ldots, s_m \mid R_1, \ldots, R_k \rangle,$$
$$\{r_1, \ldots, r_m\} \subseteq H,$$
$$\varphi : s_i \mapsto r_i \text{ be a homomorphism.}$$

If H is generated by $\{r_1, \ldots, r_m\}$ and $|H| = |G|,$ then φ is an isomorphism.

Note 19

$$D_6 \cong S_3.$$

Note 20

$D_6 \cong S_3$. What is the key idea in the proof?

▌ Build a homomorphism using the presentation of D_6.

Note 21

$D_6 \cong S_3$. Which generator of D_6 are used in the proof?

▌ r and s.

Note 22

$D_6 \cong S_3$. Which generator of S_3 are used in the proof?

▌ $a = (1\ 2)$ and $b = (1\ 2\ 3)$.

Note 23

Let $\varphi : G \to H$ be a group homomorphism. Then

$$\varphi(x^n) = \varphi(x)^n \quad \text{for all } n \in \mathbb{Z}.$$

Note 24

Let $\varphi : G \to H$ be a group homomorphism. Then

$$\varphi(x^{-1}) = \varphi(x)^{-1}.$$

Note 25

Let $\varphi : G \to H$ be a group homomorphism. Then

$$\varphi(1) = 1.$$

Note 26

Let $\varphi : G \to H$ be a group isomorphism. Then

$$\varphi(x) = 1 \iff x = 1.$$

Note 27

Let $\varphi : G \to H$ be a group homomorphism. Is it unconditionally true that $|\varphi(x)| = |x|$ for all $x \in G$?

▌ No.

Note 28

Let $\varphi : G \to H$ be a group homomorphism and G be abelian. Then

$$\varphi \text{ is surjective} \implies H \text{ is abelian.}$$

Note 29

Are the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ isomorphic?

▌ Yes.

Note 30

Are D_6 and S_3 isomorphic?

▌ Yes.

Note 31

Are the multiplicative groups $\mathbb{R}^\times$ and $\mathbb{C}^\times$ isomorphic?

▌ No.

Note 32

The multiplicative groups $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are not isomorphic. What is the key idea in the proof?

▌ $\mathbb{C}^\times$ has elements of order $n > 2$.

Note 33

Are the additive groups $\mathbb{R}$ and $\mathbb{Q}$ isomorphic?

▌ No.

Note 34

The additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic. What is the key idea in the proof?

▌ $|\mathbb{R}| \neq |\mathbb{Q}|$.

Note 35

Are the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ isomorphic?

▌ No.

Note 36

The additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. What is the key idea in the proof?

▌ $\mathbb{Q}$ has elements of order $n > 1$.

Note 37

Are D_8 and Q_8 isomorphic?

▌ No.

Note 38

D_8 and Q_8 are not isomorphic. What is the key idea in the proof?

▌ D_8 has for elements of order 2, namely s, sr, sr^2, sr^3.

Note 39

Are D_{24} and S_4 isomorphic?

▌ No.

Note 40

D_{24} and S_4 are not isomorphic. What is the key idea in the proof?

▌ D_{24} has an element of order 12.

Note 41

Let A and B be groups. Are $A \times B$ and $B \times A$ isomorphic?

▌ Yes.

Note 42

Let A, B and C be groups. Are $(A \times B) \times C$ and $A \times (B \times C)$ isomorphic?

▌ Yes.

Note 43

Let $\varphi : G \to H$ be a group homomorphism. Then {{c3::the image}} of φ is {{c1::a subgroup}} of {{c2::H.}}

Note 44

Let $\varphi : G \to H$ be a group homomorphism. If {{c2::φ is injective}} then

$$\{\{c3::G\}\}\{\{c4:: \cong \}\}\{\{c1::\varphi(G).\}\}$$

Note 45

Let $\varphi : G \to H$ be a group homomorphism. If φ is injective then $G \cong \varphi(G)$. What is the key idea in the proof?

▌ φ is surjective when its codomain is restricted to $\varphi(G)$.

Note 46

Let $\varphi : G \to H$ be a group homomorphism. {{c2::The kernel of φ}} is {{c1::the fiber of φ over 1.}}

Note 47

Let $\varphi : G \to H$ be a group homomorphism. Then {{c3::the kernel}} of φ is {{c1::a subgroup}} of {{c2::G.}}

Note 48

Let $\varphi : G \to H$ be a group homomorphism. Then φ is injective if and only if the kernel of φ is the identity subgroup of G.

Note 49

Let G be a group. Then the map $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Note 50

Let G be a group. Then the map $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Note 51

Is any surjective homomorphism necessarily an isomorphism?

❚ No.

Note 52

Let G be a group. An isomorphism from G onto G is called an automorphism of G.

Note 53

Let G be a group. The set of all automorphisms of G is denoted

$$\mathrm{Aut}(G).$$

Note 54

Let G be a group. Then $\mathrm{Aut}(G)$ is a group under function composition.

Note 55

Let G be a group. The group $(\mathrm{Aut}(G), \circ)$ is called the automorphism group of G.

Note 56

Let G be a group. A homomorphism σ such that {{c1::

$$\sigma(g) = g \text{ implies } g = 1$$

}} is called {{c2:: fixed point free.}}

Note 57

Let G be a {{c4::finite}} group. If σ is a {{c3::fixed point free}} {{c5:: automorphism}} of order {{c2::2}} in G, then

$$\sigma : x \mapsto {{c1::}} x^{-1}.}}$$

Note 58

Let G be a finite group. If σ is a fixed point free automorphism of order 2 in G, then $\sigma : x \mapsto x^{-1}$. What is the key idea in the proof?

❚ Any $g \in G$ may be expressed as $x^{-1}\sigma(x)$ for some $x \in G$.

Note 59

Let G be a finite group. If G possesses a fixed point free automorphism of order 2, then {{c1::G is abelian.}}

Note 60

Let G be a finite group. If G possesses a fixed point free automorphism of order 2, then G is abelian. What is the key idea in the proof?

❚ $\sigma : x \mapsto x^{-1}$, which is a homomorphism if and only if the group is abelian.

Note 61

Let $G = \langle x, y \rangle$ be a finite group, $x \neq y$ and $|x| = |y| = 2$. Then

$$G \cong {{c1::}} D_{2n}, }}$$

where $n = {{c2:: |xy| }}$.